### Handling Rules for Information classified as

<table>
<thead>
<tr>
<th>Classification and Labelling</th>
<th>ELECTRONIC INFORMATION</th>
<th>PHYSICAL INFORMATION</th>
<th>VERBAL INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PUBLIC</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Handling Rules for Information classified as

**GEA STRICTLY CONFIDENTIAL**

<table>
<thead>
<tr>
<th>Classification and Labelling</th>
<th>ELECTRONIC INFORMATION</th>
<th>PHYSICAL INFORMATION</th>
<th>VERBAL INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GEA STRICTLY CONFIDENTIAL</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Handling Rules for Information classified as

**GEA CONFIDENTIAL**

<table>
<thead>
<tr>
<th>Classification and Labelling</th>
<th>ELECTRONIC INFORMATION</th>
<th>PHYSICAL INFORMATION</th>
<th>VERBAL INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GEA CONFIDENTIAL</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Storage**

- Only encrypted storage combined with Digital Rights Management (DRM) is permitted.
- Do not keep unattended in your work area and store with appropriate physical security with access only to authorized personnel. The information shall be locked away in a safe. The office shall be locked outside of the working hours.

**Copying and Distribution**

- Access only to authorized personnel as well as dedicated 3rd parties and only under a confidentiality obligation. For GEA employees: Confidentiality obligation needs to be part of work contracts. For external 3rd parties: NDA with party or its organization required.
- User or entrusted person must be present during printout. A secure printing mode (incl. authentication) shall be followed. For external recipients confidentiality obligation / NDA required. Shredding via fax not allowed.

**Transmission and Transport**

- The transmission must be documented (e.g. minutes of meetings or correspondence). If possible, no external mailing. If required, only personal handover against signature in a double envelope, each glued together. The closure of the inner envelope must be signed or initialed.
- Ensure that no 3rd parties listen to your conversation. Messages containing confidential or strictly confidential information shall not be left at or answering machines, voice boxes etc. Record (e.g. in a memo or e-mail) which information was transmitted to whom – for documentation purposes. If possible, no use of any communication systems - only direct conversation in secure environment without any mobile devices in the room.

**Downgrading**

- Downgrading to PUBLIC, GEA INTERNAL or GEA CONFIDENTIAL can be performed and shall be documented. The OSG will receive an email notification. A justification for downgrading is mandatory and will be logged.
- Downgrading shall be approved by the Information Owner and the GEA CISO shall be informed. The downgrading shall be documented. Downgrading to PUBLIC shall be additionally approved by the communication department or the acceptance of the downgrading rules shall be performed and documented.

**Disposal**

- Return device to IT where it will be securely physically destroyed.
- Shredder with orders of magnitude not bigger than 30mm² or confidential waste bins.

### Handling Rules for Information classified as

**GEA INTERNAL**

<table>
<thead>
<tr>
<th>Classification and Labelling</th>
<th>ELECTRONIC INFORMATION</th>
<th>PHYSICAL INFORMATION</th>
<th>VERBAL INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GEA INTERNAL</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Storage**

- Company desktop/laptop with encrypted hard drives and corporate registered and managed mobile devices, corporate databases, and authorized cloud applications.

**Copying and Distribution**

- Only to be shared internally or with entrusted 3rd Parties (who have a need to know).

**Transmission and Transport**

- No internal restrictions for file sharing.

**Downgrading**

- Downgrading to PUBLIC can be performed and shall be documented. A justification for downgrading is mandatory and will be logged.

**Disposal**

- Return device to IT where it will be at least securely overwritten prior disposal with the intent that original data is non-retrievable.